Journal of Number Theory 132 (2012) 1295–1305

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Computing Néron–Tate heights of points on hyperelliptic Jacobians

David Holmes [1]

Institute of Mathematics, University of Warwick, Coventry CV4 7AL, United Kingdom

ARTICLE INFO

Article history:
Received 3 June 2011
Revised 5 September 2011
Accepted 9 January 2012
Available online 23 February 2012
Communicated by David Goss

MSC:
primary 14G40
secondary 11G30, 11G50, 37P30

Keywords:
Hyperelliptic curve
Canonical height
Neron–Tate height
Arakelov theory

ABSTRACT

It was shown by Faltings (1984) [Fal84] and Hriljac (1985) [Hri85] that the Néron–Tate height of a point on the Jacobian of a curve can be expressed as the self-intersection of a corresponding divisor on a regular model of the curve. We make this explicit and use it to give an algorithm for computing Néron–Tate heights on Jacobians of (hyper)elliptic curves. To demonstrate the practicality of our algorithm, we illustrate it by computing Néron–Tate heights on Jacobians of (hyper)elliptic curves of genus $1 \leqslant g \leqslant 9$.

1. Introduction

The problem considered in this paper is that of computing the Néron–Tate (or canonical) height of a point on the Jacobian of a curve of genus greater than 2. For curves of genus 1 and 2 the existing methods (classical in genus 1, and due to Flynn, Smart, Cassels and others in genus 2 [CF96] and [FS97]) make use of explicit equations for projective embeddings of Jacobians, and have proven to be very successful in practise. It does not seem practical at present to give explicit equations for Jacobians of curves of genus 3 and above (see [Stu01] and [Mue10] for recent attempts and an examination of the difficulties faced). We propose an alternative approach to computing the Néron–Tate height based on Arakelov theory. To demonstrate that our method is practical, we give numerical examples where we compute heights of points on Jacobians of (hyper)elliptic curves of genus $1 \leqslant g \leqslant 9$.

E-mail address: d.s.t.holmes@warwick.ac.uk.

[1] The author is supported by the EPSRC.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2012.01.002

The main application of these computations is at present the computation of regulators of hyperelliptic Jacobians up to rational squares; this will allow the verification of the conjectures of Birch and Swinnerton-Dyer up to rational squares. The author has also developed an algorithm to bound the difference between the naïve and Néron–Tate heights, again using Arakelov theory [Hol10]. Together, the algorithms allow a number of further applications such as computing a basis of the Mordell–Weil group of a hyperelliptic Jacobian, computing integral points on hyperelliptic curves (see [BMS+10]) and of course verifying the conjectures of Birch and Swinnerton-Dyer, up to the order of the Shafarevich–Tate group.

In this paper, curves are assumed to be smooth, projective and geometrically connected. Whilst the theoretical sections of this paper are largely independent of the curve chosen, the very geometric nature of Arakelov theory means that the details of the algorithm, and especially its implementation, will depend greatly on the geometry of the curve considered. Let C be a curve defined over a number field k. Our method makes a number of computational assumptions:

(a) We have a uniform and convenient way of representing divisor classes on the curve C.
(b) We are able to rigorously compute abelian integrals on C to any required (reasonable) precision.
(c) We are able to write down a regular proper model $\mathscr{C}$ for C over the integers $\mathcal{O}_k$ (though this need not be minimal).
(d) For each non-Archimedean place v that is a prime of bad reduction for $\mathscr{C}$, we are able to compute the intersection matrix of the special fibre $\mathscr{C}_v$.
(e) We have a way of computing Riemann–Roch spaces of divisors on C.

Assumptions (a) and (b) cause us to restrict our attention to elliptic and hyperelliptic curves. From now on we will simply refer to hyperelliptic curves, since the genus 1 case is not new; the results also apply without change to the elliptic case.

The computer algebra package MAGMA [BCP97] has in-built commands to deal with all of (a) to (e) for hyperelliptic curves over number fields. For (a), it uses Mumford's representation (see [MM84, 3.19]) for divisor classes. A MAGMA implementation by P. van Wamelen is used for integral computations in (b). This does not use the usual numerical integration techniques as these are inherently non-rigorous; instead, hyperelliptic functions are locally approximated by truncated power series and formally integrated. The computation of the intersection matrices of the special fibres at the bad places is produced by MAGMA as by-product of the computation of the regular proper model, implemented by S. Donnelly using techniques as in [Liu02, Chapter 8]. For computing Riemann–Roch spaces, MAGMA makes use of the method of Hess [Hes].

In order to simplify the exposition, we restrict our attention to curves with a rational Weierstrass point. As such, unless otherwise stated, C will denote an odd-degree hyperelliptic curve over a number field k, and $\mathscr{C}$ a proper regular—though not necessarily minimal—model of C over the integers $\mathcal{O}_k$.

The author wishes to thank Samir Siksek for introducing him to this fascinating problem, as well as for much helpful advice and a careful reading of this manuscript. Thanks are also due to Martin Bright and Jan Steffen Müller amongst others for very helpful discussions, and also to an anonymous referee for helpful suggestions.

2. A formula of Faltings and Hriljac

As before C is an odd-degree hyperelliptic curve over a number field k. We fix once and for all the following notation:

- M_k^0 the set of non-Archimedean places of k;
- M_k^∞ the set of Archimedean places of k;
- $\kappa(v)$ the residue field at a $v \in M_k^0$;
- ι_v the usual intersection pairing between divisors over $v \in M_k^0$ (see [Lan88, IV, §1]).

We shall make use of the following result which can be found in Lang's book [Lan88, IV, §2].

Theorem 1 *(Faltings and Hriljac). Let D be a degree zero divisor on C, and let E be any divisor linearly equivalent to D but with disjoint support. Then the height with respect to the ϑ-divisor of the point on* $\mathrm{Jac}(C)$ *corresponding to D is given by*

$$\hat{h}_\vartheta\big(\mathcal{O}(D)\big) = -\sum_{v\in M_k^0} \log\big|\kappa(v)\big|\iota_v\big(\overline{D}+\Phi(D),\overline{E}\big) - \frac{1}{2}\sum_{v\in M_k^\infty} g_{D,v}(E)$$

where Φ and $g_{D,v}$ are defined as follows:

– Φ sends a divisor on the curve C to an element of the group of fibral $\mathbb{Q}$-divisors on $\mathscr{C}$ with order zero along the irreducible component containing infinity, such that for any divisor D on C (with Zariski closure $\overline{D}$) and fibral divisor Y on $\mathscr{C}$, we have $\iota_v(\overline{D}+\Phi(D),Y)=0$.

– $g_{D,v}$ denotes a Green function for the divisor D, when C is viewed as a complex manifold via the embedding v.

Our strategy for computing the Néron–Tate height of a degree zero divisor D using the above formula is as follows:

(1) Determine a suitable divisor E as above. This is explained in Section 3.
(2) Determine a finite set $\mathfrak{R}\subset M_k^0$ such that for non-Archimedean places v **not** in $\mathfrak{R}$, we have $\iota_v(\overline{D}+\Phi(D),\overline{E})=0$. This is explained in Section 4.
(3) Determine $\iota_v(\Phi(D),\overline{E})$ for $v\in\mathfrak{R}$. This is explained in Section 5.
(4) Determine $\iota_v(\overline{D},\overline{E})$ for $v\in\mathfrak{R}$. This is explained in Section 6.
(5) Compute the Green function $g_{D,v}(E)$ for Archimedean v. This is explained in Section 7.

In the final section we give a number of worked examples.

By a straightforward Riemann–Roch computation, we can write down a divisor in Mumford form that is linearly equivalent to D. We replace D by this Mumford divisor. Thus we may suppose that $D = D' - d\cdot\infty$ where $d\leqslant g$ and $D' = \mathrm{zeros}(a(x), y-b(x))$ with $a(x)$, $b(x)\in k[x]$ satisfying certain conditions as given in [MM84, 3.19, Proposition 1.2].

3. Step 1: Choosing *E*

If the support of D' does not contain Weierstrass points, choose a $\lambda\in k$ such that $a(\lambda)\neq 0$, and set

$$E = \mathrm{inv}\big(D'\big) - \frac{d}{2}\,\mathrm{zeros}(x-\lambda), \tag{1}$$

where inv denotes the hyperelliptic involution. If d is odd, this is not a divisor but a $\mathbb{Q}$-divisor. This is unimportant, but if the reader is troubled he or she should multiply E by 2, and then appeal to the quadraticity of the height.

If the support of D' does contain Weierstrass points, either:
(a) replace D by a positive multiple of itself to avoid this, or
(b) add a divisor of order 2 to D to remove them.
(a) is simpler to implement, (b) generally faster computationally.

Now $E\sim_{\mathrm{lin}} -D$, and so

$$\hat{h}_\vartheta\big(\mathcal{O}(D)\big) = \sum_{v\in M_k^0} \log\big|\kappa(v)\big|\iota_v\big(\overline{D}+\Phi(D),\overline{E}\big) + \frac{1}{2}\sum_{v\in M_k^\infty} g_{D,v}(E).$$

This is seen by viewing the expression on the right hand side as the global Néron pairing on divisor classes, which is a quadratic form; since E is linearly equivalent to $-D$ a minus sign results, which cancels with those in Theorem 1 to yield the above expression.

4. Step 2: Determining a suitable $\mathfrak{R}$

We wish to find a finite set $\mathfrak{R} \subset M_k^0$ such that

$$\iota_\nu\big(\overline{D} + \Phi(D), \overline{E}\big) = 0 \tag{2}$$

for all $\nu \notin \mathfrak{R}$. To make this as general as possible, we will for the moment just assume C is a smooth curve over k in the weighted projective space $\mathbb{P}_k(a_0, \ldots, a_n)$. Let C' denote its closure in $\mathbb{P}_{\mathcal{O}_k}(a_0, \ldots, a_n)$. Let Q_1 denote the set of places of bad reduction for C', outside which C' is smooth over $\mathcal{O}_k$.

It suffices to solve our problem for prime divisors, as we can then obtain results for general D and E easily. Let X and Y be prime divisors on C, and let d be the degree of Y. Let $H_1, \ldots, H_{d+1}$ be a collection of weighted integral homogeneous forms of degrees $e_1, \ldots, e_{d+1} > 0$ on $\mathbb{P}_{\mathcal{O}_k}(a_0, \ldots, a_n)$, geometrically integral on the generic fibre and coprime over k, such that for all pairs $i \neq j$, we have on the generic fibre that $H_i \cap H_j \cap C = \emptyset$ (we will confuse H_i with the hypersurface it defines).

Let Q_2 be the set of $\nu \in M_k^0 \setminus Q_1$ such that

$$(\overline{H}_i)_\nu \cap (\overline{H}_j)_\nu \cap C'_\nu \neq \emptyset$$

for some $1 \leqslant i,\ j \leqslant d+1$. Note that $\overline{H}_i \cap \overline{H}_j$ is a zero-dimensional scheme, and so is easy to compute in practise.

Let $FF(Y)$ denote the function field of Y, a finite extension of k, and let $\mathrm{N}_Y : FF(Y) \to k$ denote the norm map. In practise, we can use Gröbner bases to find an isomorphism $FF(Y) \xrightarrow{\sim} k[t]/\alpha(t)$, and so can readily compute N_Y.

Let Q_3 be the set of $\nu \in M_k^0 \setminus (Q_1 \cup Q_2)$ such that

$$\mathrm{ord}_\nu\big(\mathrm{N}_Y\big(H_i^{e_{i+1}}/H_{i+1}^{e_i}\big)\big) \neq 0$$

for some $1 \leqslant i \leqslant d$; while Q_2 detects common points of intersection of $\overline{H}_i$, $\overline{H}_j$ and C' over ν, Q_3 detects when the intersection numbers of $\overline{H}_i^{e_i+1}$ and $\overline{H}_{i+1}^{e_i}$ with Y over ν are different.

Let $f_1, \ldots, f_r$ be integral weighted homogeneous equations for X such that no f_i vanishes on Y, and set $\deg(f_j) = d_j$. Finally let Q_4 be the set of $\nu \in M_k^0 \setminus (Q_1 \cup Q_2 \cup Q_3)$ such that

$$\mathrm{ord}_\nu\big(\mathrm{N}_Y\big(f_j^{e_1}/H_1^{d_j}\big)\big) \neq 0$$

for some $1 \leqslant j \leqslant r$.

Lemma 2. *Set*

$$\mathfrak{R} = Q_1 \cup Q_2 \cup Q_3 \cup Q_4.$$

If $\nu \notin \mathfrak{R}$ then $\iota_\nu(\overline{X} + \Phi(X), \overline{Y}) = 0$.

Proof. Outside Q_1, C' is smooth over $\mathcal{O}_k$, and hence it is regular and all its fibres are geometrically integral. As a result,

$$\iota_\nu\big(\overline{X} + \Phi(X), \overline{Y}\big) = \iota_\nu(\overline{X}, \overline{Y}) \quad \text{for } \nu \notin \mathfrak{R}. \tag{3}$$

Suppose $\iota_\nu(\overline{X}, \overline{Y}) \neq 0$, so $(\overline{X})_\nu \cap (\overline{Y})_\nu \neq \emptyset$. We will show $\nu \in \mathfrak{R}$.

Recall that X and Y are cycles on C' of relative dimension zero over $\mathcal{O}_k$, and so their fibres over closed points are cycles of dimension zero. Observe that, since the f_j are integral, we

must have $\mathrm{zeros}(f_j) \supset \overline{X}$ for all j. Hence there is some j_0 such that f_{j_0} vanishes on some irreducible component of (equivalently, closed point in) $(\overline{Y})_\nu$ (in fact, this holds for any j_0). As a result, $\iota_\nu(\mathrm{zeros}_{C'}(f_{j_0}), \overline{Y}) > 0$, since we assume $\mathrm{zeros}_{C'}(f_{j_0})$ and $\overline{Y}$ have disjoint support on the generic fibre. Now suppose $\nu \notin \mathfrak{R}$. Then for all i, since $\nu \notin Q_4$, we must have

$$\mathrm{ord}_\nu\big(\mathrm{N}_Y\big(f_{j_0}^{e_i}/H_i^{d_{j_0}}\big)\big) = 0.$$

Hence by [Lan88, III, Lemma 2.4, p. 56], we see that for all i,

$$0 = \iota_\nu\left(\mathrm{div}_{C'}\left(\frac{f_{j_0}^{e_i}}{H_i^{d_{j_0}}}\right), \overline{Y}\right) = e_i \cdot \iota_\nu\big(\mathrm{zeros}_{C'}(f_{j_o}), \overline{Y}\big) - d_{j_0} \cdot \iota_\nu\big(\mathrm{zeros}_{C'}(H_i), \overline{Y}\big).$$

Now as $e_i > 0$ and $d_{j_0} > 0$, we see that for all i,

$$\iota_\nu\big(\mathrm{zeros}_{C'}(H_i), \overline{Y}\big) > 0, \tag{4}$$

so every $\mathrm{zeros}_{C'}(H_i)$ meets $\overline{Y}$. But the zero-dimensional cycles $\mathrm{zeros}_{C'}(H_i) \cap \overline{Y}$ are pairwise disjoint since $\nu \notin Q_2$, and $\deg(Y) = \deg((\overline{Y})_\nu) = d$. Moreover, $\nu \notin Q_3$ shows that the $(d+1)$ cycles $\mathrm{zeros}(H_i) \cap \overline{Y}$ are disjoint, and so cannot all meet the zero-dimensional cycle $(\overline{Y})_\nu$ as it has degree d; this contradicts Eq. (4), and so we are done. □

5. Step 3: Determining $\iota_\nu(\Phi(D), \overline{E})$

We next discuss the computation of the term $\iota_\nu(\Phi(D), \overline{E})$ for a non-Archimedean place ν. Recall that by our assumptions in Section 2 we are able to write down a proper regular model $\mathscr{C}$ and the intersection matrix for $\mathscr{C}_\nu$ for all bad places ν. Clearly $\iota_\nu(\Phi(D), \overline{E})$ vanishes if $\mathscr{C}_\nu$ is integral, in particular if ν is a good prime. Suppose ν is a bad prime. Since we have the intersection matrix of $\mathscr{C}_\nu$, we can easily compute both $\Phi(D)$ and $\iota_\nu(\Phi(D), \overline{E})$ from the definition of Φ if we can solve the following:

Problem 3. Given a finite place ν, a horizontal divisor X and a prime fibral divisor Y over ν, compute $\iota_\nu(X, Y)$.

We may replace the base space $S = \mathrm{Spec}(\mathcal{O}_k)$ by its completion $\hat{S}$ at ν [Lan88, III, Proposition 4.4, p. 65], and we may further assume that X is a prime horizontal divisor on $\mathscr{C} \times_S \hat{S}$. By Lemma 4 below, this means that the support of X_ν is a closed point of $\mathscr{C}_\nu$, and so we can find an affine open neighbourhood $U = \mathrm{Spec}(A)$ of X_ν in $\mathscr{C} \times_S \hat{S}$.

Lemma 4. *If X is a prime horizontal divisor on $\mathscr{C} \times_S \hat{S}$, then the support of X_ν is a prime divisor on $\mathscr{X}_\nu$ (in other words, X_ν is irreducible but not necessarily reduced).*

Proof. There exist a number field L and an order R in L such that X is isomorphic to $\mathrm{Spec}(R)$. Write $L = k[t]/\alpha(t)$, where α monic and irreducible with integral coefficients. Let κ denote the residue field of k, and $\overline{\alpha}$ the image of α in $\kappa[t]$. If X_ν is not irreducible, then there exist f, $g \in \kappa[t]$ coprime monic polynomials such that $f \cdot g = \overline{\alpha}$. This factorisation of $\overline{\alpha}$ lifts to a factorisation of α by Hensel's lemma. □

Now it is easy to check whether $X_\nu \cap Y = \emptyset$; if so, $\iota_\nu(X, Y) = 0$. Further, if $X_\nu \subset Y$ and X_ν is not contained in any other fibral prime divisor, then $\iota_\nu(X, Y) = \deg(X)$; this is easily seen since locally $Y = \mathrm{zeros}_U(\nu)$, and we can take the norm of ν from the field of fractions $FF(X)$ down to k.

We are left with the case where X_ν lies at the intersection of several fibral prime divisors. Recall that X is assumed to be horizontal. We find equations $\overline{f}_1, \ldots, \overline{f}_r \in A \otimes_{\mathcal{O}_k} \kappa(\nu)$ for Y as a subscheme of U_ν. Then choose any lifts f_i of $\overline{f}_i$ to A. Now we need two easy results in commutative algebra:

Lemma 5. *Let R be a ring, $p \in R$ any element, and I an ideal containing p. Suppose we have $t_1, \ldots, t_r \in R$ such that the images $\bar{t}_1, \ldots, \bar{t}_r$ in $R/(p)$ generate the image of I in $R/(p)$. Then $I = (t_1, \ldots, t_r, p)$.*

Proof. Let $x \in I$. Write $\bar{x}$ for the image of x in $R/(p)$, and write $\bar{x} = \sum_{i=1}^r \bar{\alpha}_i \bar{t}_i$ for some $\bar{\alpha} \in R/(p)$. Choose lifts α_i of $\bar{\alpha}_i$ to R. Then $y \stackrel{\text{def}}{=} x - \sum_{i=1}^r \alpha_i t_i$ has the property that $y \in p \cdot R$. Hence x is in $(t_i, \ldots, t_r, p)$ and so $I \subset (t_1, \ldots, t_r, p)$. Now $p \in I$ by assumption, and $\bar{t}_i \in I/(p)$, so there exists g_i in I such that $g_i - t_i \in p \cdot R$, so $t_i \in I$. □

Lemma 6. *Let R be a regular local ring, and $t_1, \ldots, t_r \in R$ be such that $I \stackrel{\text{def}}{=} (t_1, \ldots, t_r)$ is a prime ideal of height* 1. *Now I is principal; write $I = (t)$. Then there exist an index i and a unit $u \in R$ such that $t_i = tu$. In particular, there exists an index i with $I = (t_i)$.*

Proof. R is a unique factorisation domain, and so for each i we can write $t_i = t_i' t$ for some $t_i' \in R$. Hence $I = t \cdot (t_1', \ldots, t_r')$, and $(t_1', \ldots, t_r') = 1$. We want to show some t_i' is a unit. Suppose not; then since A is local, all the t_i' lie in the maximal ideal, so $(t_1', \ldots, t_r')$ is contained in the maximal ideal, a contradiction. □

Now from these we see that one of the f_i or ν must be an equation for Y in a neighbourhood of X_ν (and it cannot be ν as X_ν lies on an intersection of fibral primes). Now if any f_i vanishes on X_ν, it cannot be the f_i we seek. Exclude such f_i, and then for each of the remaining f_i compute its norm from $FF(X)$ to the completion of k. The minimum of the valuations of such norms will be achieved by any f_i which is a local equation for Y at X_ν, and hence $\iota_\nu(Y, X)$ is equal to the minimum of the valuations of the norms.

6. Step 4: Determining $\iota_\nu(\overline{D}, \overline{E})$

Finally, we come to what appears to be the meat of the problem for non-Archimedean places: given two horizontal divisors D and E and a place $\nu \in \mathfrak{R}$, compute the intersection $\iota_\nu(\overline{D}, \overline{E})$. However, the techniques used in previous sections actually make this very simple.

Fix a non-Archimedean place ν. Let $\hat{S}$ denote the ν-adic completion of S, and set $\hat{\mathscr{C}} = \mathscr{C} \times_S \hat{S}$. It is sufficient to compute the intersection $\iota_\nu(X, Y)$ where X and Y are prime horizontal divisors on $\hat{\mathscr{C}}$; in particular (by Lemma 4), the supports of X_ν and Y_ν are closed points of $\mathscr{C}_\nu = \hat{\mathscr{C}}_\nu$

Now if $\mathrm{Supp}(X_\nu) \neq \mathrm{Supp}(Y_\nu)$, then $\iota_\nu(X, Y) = 0$. Otherwise, let $U = \mathrm{Spec}(A)$ be an affine open neighbourhood of $\mathrm{Supp}(X_\nu)$. Let $f_1, \ldots, f_r$ generate the ideal of X on U; then by Lemma 6 we know that some f_i generates the ideal of X in a neighbourhood of X_ν. If f_j vanishes on Y, we can throw it away. We obtain

Proposition 1.

$$\iota_\nu(X, Y) = \min_i \big(\mathrm{ord}_\nu\big(f_i[Y]\big)\big)$$

as i runs over $\{1, \ldots, r\}$ such that f_i does not vanish identically on Y_ν. Here $f[Y]$ is defined to be either

(1) *the norm from $FF(Y)$ to the completion of k of the image of f_i in $FF(Y)$, or, equivalently,*
(2) *$\prod_j f_i(p_j)^{n_j}$ where $Y = \sum_j n_j p_j$ over some finite extension l/k (see* [Lan88, II, §2, p. 57]*).*

Proof. If f_i is not identically zero on Y_v, then $\mathrm{zeros}_{\hat{\mathscr{C}}}(f_i)$ and Y have no common component and moreover f_i is regular on a neighbourhood of Y so $\iota_v(\mathrm{poles}_{C'}(f_i), Y) = 0$, and so [Lan88, II, Lemma 24, p. 56] shows that

$$\iota_v\big(\mathrm{zeros}_{\hat{\mathscr{C}}}(f_i), Y\big) = \mathrm{ord}_v\big(f_i[Y]\big). \tag{5}$$

Now $\mathrm{zeros}_{\hat{\mathscr{C}}}(f_i) \geqslant X$, so $\mathrm{ord}_v(f_i[Y]) \geqslant \iota_v(X, Y)$. Moreover, by Lemma 5 there is an index i_0 such that f_{i_0} generates X near X_v, and since $X_v = Y_v$ is irreducible we have that

$$\begin{aligned}\iota_v(X, Y) = \iota_v\big(\mathrm{zeros}_{\hat{\mathscr{C}}}(f_{i_0}), Y\big) &= \sum_p \mathrm{length}_{\mathcal{O}_p}\left(\frac{\mathcal{O}_p}{f_{i_0}, I_Y}\right) \\ &= \mathrm{length}_{\mathcal{O}_{X_v}}\left(\frac{\mathcal{O}_{X_v}}{f_{i_0}, I_Y}\right)\end{aligned} \tag{6}$$

where the sum is over closed points p of $\hat{\mathscr{C}}$ lying over v, and I_Y is the defining ideal for Y in the local ring under consideration. Now any other f_i will have

$$\iota_v\big(\mathrm{zeros}_{\hat{\mathscr{C}}}(f_i), Y\big) \geqslant \iota_v\big(\mathrm{zeros}_{\hat{\mathscr{C}}}(f_{i_0}), Y\big), \tag{7}$$

so the result follows. □

As regards the computation of the $f_i[Y]$, definitions (1) and (2) given in Proposition 1 lead to slightly different approaches, but both make use of Pauli's algorithms [PR01]. In our implementation, discussed in Section 8, we use (2) as it seems easier; however (1) may lead to an implementation that is faster in practise.

7. Step 5: Computing $g_{D,v}(E)$

Finally, we must compute the Archimedean contribution. Fix for the remainder of this section an embedding σ of k in $\mathbb{C}$ corresponding to a place $v \in M_k^\infty$. Let C_σ denote the Riemann surface corresponding to $C \times_{k,\sigma} \mathbb{C}$.

7.1. The PDE to be solved

As a starting point, we take [Lan83, Chapter 13, Theorem 72], which we summarise here.

Given a divisor a on C_σ of degree zero, let ω be a differential form on C_σ such that the residue divisor $\mathrm{res}(\omega)$ equals a (such an ω can always be found using the Riemann–Roch theorem). Normalise ω by adding on holomorphic forms until the periods of ω are purely imaginary. Let

$$dg_a \stackrel{\mathrm{def}}{=} \omega + \overline{\omega}. \tag{8}$$

Then g_a is a Green function for a. Thus it remains to find, normalise and integrate such a form ω.

7.2. Application of theta functions to the function theory of hyperelliptic curves

We can use ϑ-functions to solve the partial differential equation (8) of Section 7.1, in a very simple way. For background on ϑ-functions we refer to the first two books of the 'Tata lectures on theta' trilogy [Mum83], [MM84]. ϑ-functions are complex analytic functions on $\mathbb{C}^g$ which satisfy some quasi-periodicity conditions, thus they are an excellent source of differential forms on the (analytic) Jacobian of C_σ. To get from this a differential form on C_σ we simply use that C_σ is canonically embedded in $\mathrm{Jac}(C_\sigma)$ by the Abel–Jacobi map, so we can pull back forms from $\mathrm{Jac}(C_\sigma)$ to C_σ.

Fix a symplectic homology basis A_i, B_i on C_σ as in [MM84]; by this we mean that if $i(-,-)$ denotes the intersection of paths, then we require that the A_i, B_i form a basis of $H_1(C_\sigma, \mathbb{Z})$ such that

$$i(A_i, A_j) = i(B_i, B_j) = 0 \quad \text{for } i \neq j$$

and

$$i(A_i, B_j) = \delta_{ij}.$$

We also choose a basis $\omega_1, \ldots, \omega_g$ of holomorphic 1-forms on C_σ, normalised such that

$$\int_{A_i} \omega_j = \delta_{ij}.$$

We recall the definition and some basic properties of the multivariate ϑ-function:

$$\vartheta(z; \Omega) \stackrel{\text{def}}{=} \sum_{\underline{n} \text{ in } \mathbb{Z}^g} \exp\left(\pi i \underline{n} \Omega \underline{n}^{\mathrm{T}} + 2\pi i \underline{n} \cdot z\right) \tag{9}$$

which converges for z in $\mathbb{C}^g$ and Ω a $g \times g$ symmetric complex matrix with positive definite imaginary part. The ϑ-function satisfies the following periodicity conditions for $\underline{m}, \underline{n}$ in $\mathbb{Z}^g$:

$$\vartheta(z + \underline{m}; \Omega) = \vartheta(z; \Omega), \tag{10}$$

$$\vartheta(z + \underline{n}\Omega; \Omega) = \exp\left(-\pi i \underline{n} \Omega \underline{n}^{\mathrm{T}} - 2\pi i \underline{n} z\right) \vartheta(z; \Omega). \tag{11}$$

We will set Ω to be the period matrix of the analytic Jacobian of C_σ with respect to the fixed symplectic homology basis (as in [MM84]), and z will be a coordinate on the analytic Jacobian. This means that

$$\Omega_{ij} = \int_{B_i} \omega_j.$$

Let

$$\delta' \stackrel{\text{def}}{=} \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}, \frac{1}{2}\right) \in \frac{1}{2}\mathbb{Z}^g,$$

$$\delta'' \stackrel{\text{def}}{=} \left(\frac{g}{2}, \frac{g-1}{2}, \ldots, 1, \frac{1}{2}\right) \in \frac{1}{2}\mathbb{Z}^g,$$

$$\Delta \stackrel{\text{def}}{=} \Omega \cdot \delta' + \delta''.$$

Then [MM84, Theorem 53, part 1] tells us that $\vartheta(\Delta - z) = 0$ if and only if there are $P_1, \ldots, P_{g-1}$ in C_σ such that

$$z \equiv \sum_{i=1}^{g-1} \int_\infty^{P_i} \underline{\omega} \pmod{\mathbb{Z}^g + \Omega\mathbb{Z}^g}.$$

This is a crucial result which allows us to construct a quasifunction on $\mathrm{Jac}(C_\sigma)$ with prescribed zeros, and from this obtain the Green function we seek.

7.3. Solution of the partial differential equation

Let D, D_0 be two effective reduced divisors of degree g on C_σ with disjoint support, containing no Weierstrass points or points at infinity, nor any pairs $p+q$ of points such that $p = \mathrm{inv}(q)$. Then the classes $[\mathcal{O}(D - g\cdot\infty)]$ and $[\mathcal{O}(D_0 - g\cdot\infty)]$ lie outside the ϑ-divisor on the Jacobian; indeed, the association $D \mapsto [\mathcal{O}(D - g\cdot\infty)]$ is an isomorphism from divisors with the above properties to $\mathrm{Jac}(C_\sigma)\setminus\vartheta$, see [MM84, 331]. Write $\alpha : \mathrm{Div}(C_\sigma) \to \mathrm{Jac}(C_\sigma)$ for the map sending a divisor E to the class $[\mathcal{O}(E - \deg(E)\cdot\infty)]$.

For z in $\mathrm{Jac}(C_\sigma)$ we set

$$G(z) = \frac{\vartheta(z + \Delta - \alpha(D))}{\vartheta(z + \Delta - \alpha(D_0))}.$$

Then for p in C_σ we set $F(p) = G(\alpha(p))$ so

$$F(p) = \frac{\vartheta(\alpha(p) + \Delta - \alpha(D))}{\vartheta(\alpha(p) + \Delta - \alpha(D_0))}. \tag{12}$$

If we let $\omega = d\log F(p)$ then it is clear that $\mathrm{res}(\omega) = D - D_0$. It then remains to normalise ω to make its periods purely imaginary, and then integrate it. We have a homology basis A_i, B_i, and we find:

$$\int_{A_k} \omega = \int_{A_k} d\log F(p) = \log G\big(\alpha(p) + e_k\big) - \log G\big(\alpha(p)\big) = 0$$

(where $e_k = (0, 0, \ldots 0, 1, 0 \ldots, 0)$ with the 1 being in the k-th position), and

$$\begin{aligned}\int_{B_k} \omega = \int_{B_k} d\log F(p) &= \log G\big(\alpha(p) + \Omega.e_k\big) - \log G\big(\alpha(p)\big)\\ &= 2\pi i e_k^T \cdot \big(\alpha(D) - \alpha(D_0)\big).\end{aligned}$$

From this we can deduce that the normalisation is

$$\begin{aligned}\omega = d\log&\left[\frac{\vartheta(\alpha(p) + \Delta - \alpha(D))}{\vartheta(\alpha(p) + \Delta - \alpha(D_0))}\right]\\ &- 2\pi i\Big[\big(\mathrm{Im}(\Omega)\big)^{-1}\,\mathrm{Im}\big(\alpha(D) - \alpha(D_0)\big)\Big]\cdot\begin{bmatrix}\omega_1\\ \omega_2\\ \vdots\\ \omega_g\end{bmatrix}\end{aligned}$$

where p is a point on C_σ.

Now we integrate to get the Green function $g_{D-D_0}(p) = \int_{\infty_{C_\sigma}}^{p} \omega + \overline{\omega}$, where ∞_{C_σ} denotes the point at infinity on C_σ:

$$g_{D-D_0}(p) = 2\log\left|\frac{\vartheta(\alpha(p) + \Delta - \alpha(D))}{\vartheta(\alpha(p) + \Delta - \alpha(D_0))}\right|$$

$$+ 4\pi\left[\left(\operatorname{Im}(\Omega)\right)^{-1}\operatorname{Im}\left(\alpha(D)-\alpha(D_0)\right)\right]\cdot\operatorname{Im}\left(\int_{\infty_{C_\sigma}}^{p}\begin{bmatrix}\omega_1\\ \omega_2\\ \vdots\\ \omega_g\end{bmatrix}\right)$$

$$= 2\log\left|\frac{\vartheta(\alpha(p)+\Delta-\alpha(D))}{\vartheta(\alpha(p)+\Delta-\alpha(D_0))}\right| + 4\pi\left(\operatorname{Im}(\Omega)\right)^{-1}\cdot\operatorname{Im}\left(\alpha(D)-\alpha(D_0)\right)\cdot\operatorname{Im}\left(\alpha(p)\right).$$

Given divisors D, D_0 and E, E_0 containing no Weierstrass points or infinite points or pairs of points which are involutions of each other, and having disjoint support we can this formula to compute $\frac{1}{2}g_{D-D_0}[E-E_0]$ which is simply the sum over points $p\in\operatorname{Supp}(E-E_0)$ of $g(p)$. We are done.

8. Examples

We have created a test implementation of the above algorithm in MAGMA. The following results were obtained using a 2.50 GHz Intel Core2 Quad CPU Q9300:

First, we let $C/\mathbb{Q}$ be the genus 3 hyperelliptic curve given by

$$C\colon y^2 = x^7 - 15x^3 + 11x^2 - 13x + 25.$$

Let D, E be the points on the Jacobian corresponding to the degree 0 divisors $(1,3)-\infty$, $E=(0,-5)-\infty$ respectively. We obtain the following:

$$\hat{h}(D) = 1.77668\ldots,$$
$$\hat{h}(E) = 1.94307\ldots,$$
$$\hat{h}(D+E) = 4.35844\ldots,$$
$$\hat{h}(D-E) = 3.08107\ldots,$$
$$2\hat{h}(D)+2\hat{h}(E)-\hat{h}(D+E)-\hat{h}(D-E) = 1.26217\times 10^{-28}$$

with a total running time of 31.75 seconds. We note that our result is consistent with the parallelogram law for the Néron–Tate height, which provides a useful check that our implementation is running correctly.

Next we give two families of curves of increasing genus. Firstly the family $y^2 = x^{2g+1}+2x^2-10x+11$ with D denoting the point on the Jacobian corresponding to the degree 0 divisor $(1,2)-\infty$ (all times are in seconds unless otherwise stated):

g	$\hat{h}(D)$	time
1	1.11466...	1.94
2	1.35816...	6.44
3	1.50616...	15.10
4	1.61569...	32.71
5	63.4292...	72.23
6	1.77778...	212.37
7	51.0115...	20 minutes
8	1.89845...	3 hours
9	78.8561...	16 hours

Now we consider the family $y^2 = x^{2g+1}+6x^2-4x+1$ with D denoting the point $(1,2)+(0,1)-2\cdot\infty$ on the Jacobian:

g	$\hat{h}(D)$	time/seconds
1	1.41617...	2.06
2	1.37403...	6.73
3	1.50396...	15.62
4	1.40959...	32.60
5	1.70191...	76.48
6	1.81093...	291.17
7	1.71980...	1621.50

A fully-functioning and more efficient implementation of Néron–Tate height computations is currently being carried out in MAGMA by J.S. Müller, combining ideas from this paper with those from his own PhD thesis [Mue10]. Müller's approach to computing $\iota_v(D, E)$ is quite different from that used here; he uses Gröbner bases to compute directly the $\mathcal{O}_p$-length of the modules $\frac{\mathcal{O}_p}{I_D+I_E}$ as p runs over closed points of the special fibre, in contrast to the method in this paper where we compute norms down to the ground field and then compute valuations.

References

[BCP97] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory, London, 1993, J. Symbolic Comput. 24 (3–4) (1997) 235–265. .

[BMS+10] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, Sz. Tengely, Integral points on hyperelliptic curves, preprint, 2010.

[CF96] J.W.S. Cassels, E.V. Flynn, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, London Math. Soc. Lecture Note Ser., vol. 230, Cambridge University Press, Cambridge, 1996.

[Fal84] G. Faltings, Calculus on arithmetic surfaces, Ann. of Math. 119 (2) (1984) 387–424.

[FS97] E.V. Flynn, N.P. Smart, Canonical heights on the Jacobians of curves of genus 2 and the infinite descent, Acta Arith. 79 (4) (1997) 333–352.

[Hes] F. Hess, Computing Riemann–Roch spaces in algebraic function fields and related topics, J. Symbolic Comput. 33 (2002) 425–445.

[Hol10] D. Holmes, Heights on high-genus hyperelliptic curves, University of Warwick PhD thesis, 2012, in preparation.

[Hri85] P. Hriljac, Heights and Arakelov's intersection theory, Amer. J. Math. 107 (1) (1985) 23–38.

[Lan83] S. Lang, Fundamentals of Diophantine Geometry, Springer-Verlag, New York, 1983.

[Lan88] S. Lang, Introduction to Arakelov Theory, Springer, 1988.

[Liu02] Q. Liu, Algebraic Geometry and Arithmetic Curves, Oxf. Grad. Texts Math., vol. 6, Oxford University Press, Oxford, 2002. Translated from French by Reinie Erné, Oxford Science Publications.

[MM84] D. Mumford, C. Musili, Tata Lectures on Theta: Jacobian Theta Functions and Differential Equations, Springer, 1984.

[Mue10] J.S. Mueller, Computing canonical heights using arithmetic intersection theory, eprint arXiv:1105.1719, 2011.

[Mum83] D. Mumford, Tata Lectures on Theta I, Birkhäuser, 1983.

[PR01] S. Pauli, X.F. Roblot, On the computation of all extensions of a p-adic field of a given degree, Math. Comp. 70 (236) (2001) 1659.

[Stu01] A.G.J. Stubbs, Hyperelliptic Curves, 2001.